

Usage Guidelines for AI Tools at the Weizmann Institute

The tools approved by the Weizmann IT are part of the Edu track, which means that the learning option of the tool is disabled, and all data remains strictly within the organization.

Below are general usage guidelines for AI tools that are not centrally managed by Weizmann IT.

1. **Extreme caution must be exercised when uploading information and materials to AI tools.**

The institute is committed to maintaining high standards of information security and ensuring the confidentiality of its own data and materials, as well as those of third parties, including preventing their misuse.

When using AI tools, which are services managed by third parties, it should be assumed that any uploaded data may be exposed to external entities and, in some cases, may be used for training AI models. Therefore, **sensitive or confidential information should not be uploaded to any AI tool, including but not limited to: large amounts of personal data, passwords, proprietary source code, information about the institute's computing infrastructure, sensitive financial data, information protected under confidentiality agreements, medical or biometric data**. Before uploading any data to AI tools, it must be classified according to its sensitivity level, and preference should be given to using public or general information. If there is any doubt about the sensitivity of the information, it should not be uploaded, and the relevant authorities at the institute should be consulted. In any case of suspected exposure of confidential or sensitive information, it must be reported immediately to the Information Security Section at Weizmann IT.

2. **Using AI Tools Outside Institute-Provided Accounts**

When using AI tools that have not been officially provided by the institute, it is important to understand that the institute has no agreements, affiliations, or control over their operation, data security measures, or the way they process and use uploaded information. Therefore, it is strictly prohibited to upload or provide: personal data (any information that identifies or could identify an individual), proprietary information, confidential or sensitive information belonging to the institute or third parties to any external AI tools. Additionally, AI tools that have not been approved by the institute must not be installed on the institute's computers.

3. **AI Tools as a Supportive Aid Only**

The use of AI tools within the institute is intended solely as a supportive aid and not as a substitute for professional work. This is because the data sources and materials on which many AI tools rely are not transparent, and there is no certainty regarding the reliability or origin of their outputs. Therefore, AI tools should not be relied upon to generate complete outputs such as agreements, articles, or full text segments. Extra caution should be taken when integrating AI-generated content (such as text, computer code, images, voice

recordings, or other visual materials) into the institute's products, services, or publications. Every output must be the result of professional work, with AI tools used solely for support, inspiration, and process efficiency. Under no circumstances should AI-generated work be presented as original work.

4. **AI Tools Must Not Be Used for Decision-Making Regarding Individuals**

AI tools may exhibit biases, and their decision-making capabilities are not equivalent to human judgment. Therefore, it is strictly prohibited to rely on AI tools for making decisions that affect people.

5. **Responsible and Transparent Use of AI Tools**

AI tools represent new and evolving technology, and their outputs and the consequences of their use may be unpredictable. Users must exercise judgment, responsibility, and transparency in every action involving AI tools and in every use of their outputs.